H3C

RISING 瑞星

H3C ASM 防病毒卡 用户手册

杭州华三通信技术有限公司

http://www.h3c.com.cn

北京瑞星科技股份有限公司

http://www.rising.com.cn

资料版本：20080310-C-1.00

声明

H3C、**H3C**、Aolynk、Aolynk、H^{3}Care、、TOP G、TOPG、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V^{2}G、V^{n}G、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。如需要获取最新手册，请登录 http://www.h3c.com.cn

感谢您购买 H3C 公司的 ASM 防病毒卡。请在使用本产品之前认真阅读配套的使用手册。当您开始使用本产品时，H3C 公司认为您已经阅读了本手册。

作为计算机病毒清除工具和网络安全防护工具，针对网络的不断变化，H3C 公司研制销售的 ASM 防病毒卡将不断地升级。无论是功能的增加、性能的提高，还是清除病毒种类的增加都关系到其实际的使用效果。因此，您在使用本产品过程中应随时对产品进行升级。

随着产品不断升级，本手册的内容将会有所更改，恕不另行通知。您可以从网站 http://www.h3c.com下载到手册的最新版本。

ASM 防病毒卡上的瑞星防毒墙软件的知识产权归北京瑞星科技股份有限公司所有。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

目录

前 言

在网络技术和网络设备不断发展的今天，网络安全问题正日益变得重要。如何使网络和主机不受病毒的入侵，已经成为网络建设和应用部署过程中迫切需要解决的问题。对于病毒的防范和隔离，过去常规的做法是在主机上安装防病毒软件。大部分病毒威胁是来自于外网的，而在各个主机上安装防病毒软件虽然能防止病毒对本机的攻击，但并不能阻止病毒在网络上的传播。

在这种背景下，防病毒卡应运而生。它通过网络设备来防范和隔离病毒，在网关处就对病毒进行有效地查杀，很好地弥补了防毒软件的不足，具有很强的可用性和可部署的能力。

H3C公司和国内著名的防病毒厂商瑞星合作，基于H3C公司的OAA（Open Application Architecture）架构，推出了ASM（Anti-Virus Security Module）防病毒卡。该卡通过将瑞星企业级防毒引擎集成到网络产品的OAP模块中来提供查杀病毒的功能。

H3C公司的开放式业务平台OAP模块具有强大的处理能力和独特灵活的业务集成能力，而瑞星公司的防病毒产品的功能和性能在业界是首屈一指的。因此，ASM防病毒卡解决方案是强强联合的结晶，不论是品牌还是功能和性能方面都具有很强的优势。

第一章 产品简介

1.1 技术特点

ASM 防病毒卡是基于 H3C 公司的 OAA 架构进行设计的。

OAA 架构是 H3C 公司提出的一套完整的软硬件接口及标准规范。它提供了一个开放平台，第三方厂商在此基础上可开发出更为丰富的业务，从而发挥各个厂家在各自领域的优势，同时也降低了用户投资。

防病毒产品适用于各类复杂的网络环境，具有灵活的配置管理方式，集成瑞星最新的 VUE 杀毒引擎、未知病毒查杀技术、详细的日志分析等多个模块，方便管理、易于操作、查杀病毒准确快速，为用户提供了一套完整的信息安全解决方案。

综上所述，采用了 OAA 架构的 ASM 防病毒卡功能强大，可以安装在 H3C 公司生产的多种网络设备上。

1.2 ACFP 介绍

在 OAA 架构中，ASM 防病毒卡和网络设备互相协作，共同完成查杀病毒的任务。这两者的协作过程是由 ACFP 联动规范定义的。

ACFP（Application control forward protocol）即应用控制转发协议，是一种设备间的 C/S（客户端/服务端）模式的联动框架。它主要描述了 ASM 防病毒卡和 H3C 公司的网络设备之间联动的具体实现规范。ASM 防病毒卡被称为 ACFP Client，网络设备被称为 ACFP Server。

根据报文通过 ACFP Server 和 ACFP Client 的方式，ACFP 联动的工作模式分为以下四类：主机模式、透传模式、镜像模式和重定向模式。

ASM 防病毒卡的工作模式是重定向模式，如图所示：

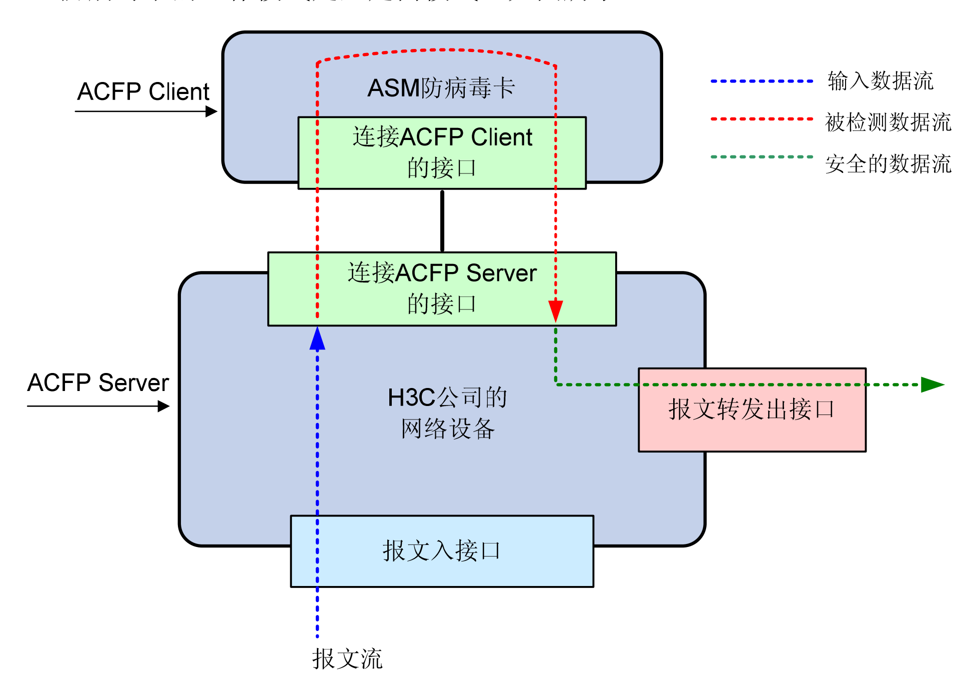


图 1.1 重定向模式示意图

1.3 杀毒软件工作原理

下面是运行在防病毒卡上的杀毒软件的工作原理图：

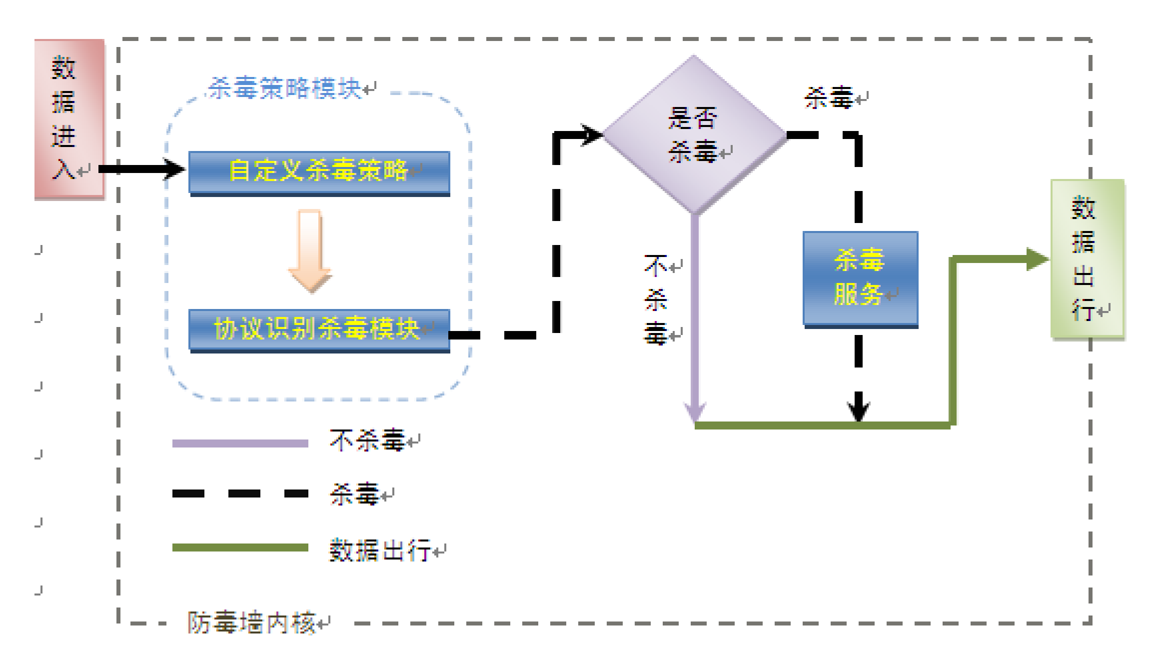


图 1.2 杀毒软件工作原理

杀毒软件读取数据后，首先进行自定义杀毒策略规则匹配，如果符合自定义杀毒策略则转交协议识别模块的协议匹配，如果不符合自定义杀毒策略则直接进行数据包转发。当数据包转交到协议识别模块时，会进行协议检查，如果属于防毒引擎支持的协议则进行杀毒，反之，则直接进行数据转发。

1.4 组网应用

ASM 防病毒卡可以在 H3C 公司的新一代网络设备上应用，前景十分广阔。如：

- 大中型企业和中小型企业网络；
- 各种病毒泛滥的网吧、园区网络的入口；
- 企业网络的 intranet 及其分支机构的接入口。

下面是一张典型组网示意图。装有 ASM 防病毒卡的网络设备可以分别作为总部和分支各自的网络的入口设备，起到查杀病毒的作用。

这种防病毒卡和网络设备的融合无疑是一种非常实用的网络安全解决方案。

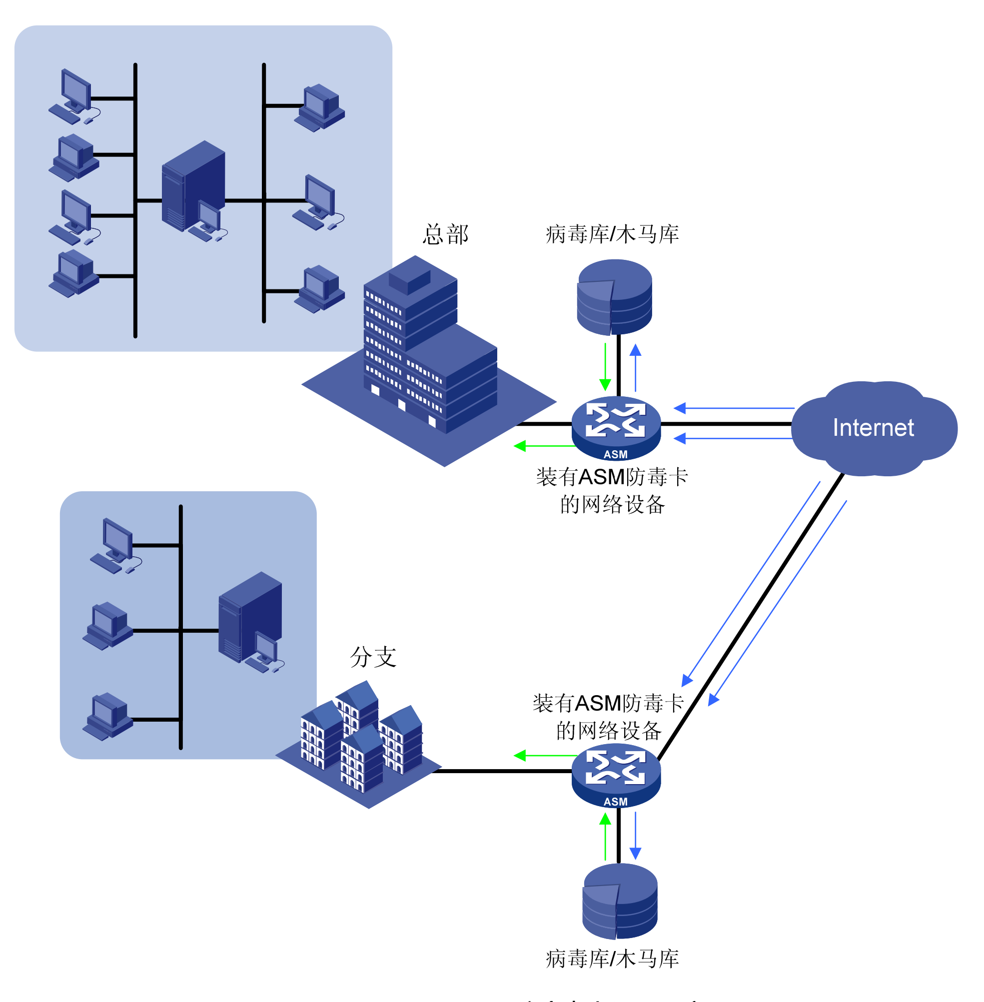


图 1.3 ASM 防病毒卡组网示意图

1.5 防病毒卡优点

ASM 防病毒卡可以很好地防御目前流行的混合型数据攻击，有效的减少内部网络不必要的带宽浪费。通过 ASM 防病毒卡，管理员可以很容易地防御外部网络的蠕虫攻击、木马进程和垃圾邮件的侵袭，有效地保护了内部网络；同时阻断来自内部的数据攻击以及垃圾数据流的泛滥，有效地控制和防范病毒在外部网络上的传播。

防病毒卡的主要优点还有：

- 防病毒卡部署在网络设备上，配合在每一台主机上安装的防病毒软件，二者共同进行查杀病毒的任务，显著提高了杀毒效率
- 防病毒卡使用专门的硬件平台。它既不占用网络设备的硬件资源，也不影响网络设备的性能，保证了网络设备的正常工作和数据转发。另外，防病毒卡集成在网络设备里，通过网络设备来进行管理和配置，方便了用户的使用
- 完善的安全审计。提供了完整的日志记录及审计功能，可提供详细的日志分析统计报告，帮助管理员发现网络被入侵的痕迹，以便及时采取弥补措施，或追踪入侵者
- 灵活的设置。提供针对 HTTP、FTP、SMTP、POP3 四种协议的数据流进行查毒和杀毒的功能，可以分为按文件大小、性能优先或者准确性优先、文件类型、自定义策略等等各种条件进行查杀病毒，满足用户多种需求
- 病毒特征库支持动态更新，具有自动升级和手动升级两种方式，保证了杀毒引擎对新型病毒的查杀。

第二章 登录防病毒卡管理界面

防病毒卡提供两种设置模式：串口命令行模式（串口命令行模式的说明见附录一串口管理）和Web图形化界面模式。本章主要介绍Web图形化界面模式下如何登录防病毒卡并对防病毒卡进行管理操作。主要包括：

- 登录防病毒卡前的准备工作
- 登录防病毒卡
- 防病毒卡功能菜单

2.1 登录防病毒卡前的准备工作

建议用户使用 Internet Explorer 6.0 或更高版本浏览器。

为了创建一个到您的工作站的安全连接，防病毒卡使用了安全套接层（SSL）协议（2.0 或 3.0 版本）。在防病毒卡连接期间，所有的交换信息均被 SSL 加密，默认的访问端口为 443。

为了保证您能够访问防病毒卡的web管理界面，您的计算机必须有一个与防毒墙管理口在同一网段内的IP地址。（关于防病毒卡的三个IP地址的含义，请参见3.2.1 防病毒卡接口配置 ）

防病毒卡出厂信息	
管理接口 IP 地址：192.168.2.1	网络掩码：255.255.255.0
本地 IP 地址：192.168.1.1	网络掩码：255.255.255.255
关联 IP 地址：192.168.1.2	网络掩码：255.255.255.255
登录用户名：admin	登录密码：admin

表 1 防病毒卡出厂信息

默认情况下应将管理计算机 IP 地址设置为 192.168.2.*（*为 2~254 的任意数字，这里我们用 100 为例），子网掩码为 255.255.255.0，默认网关为 192.168.2.1。如图 2.1 所示。

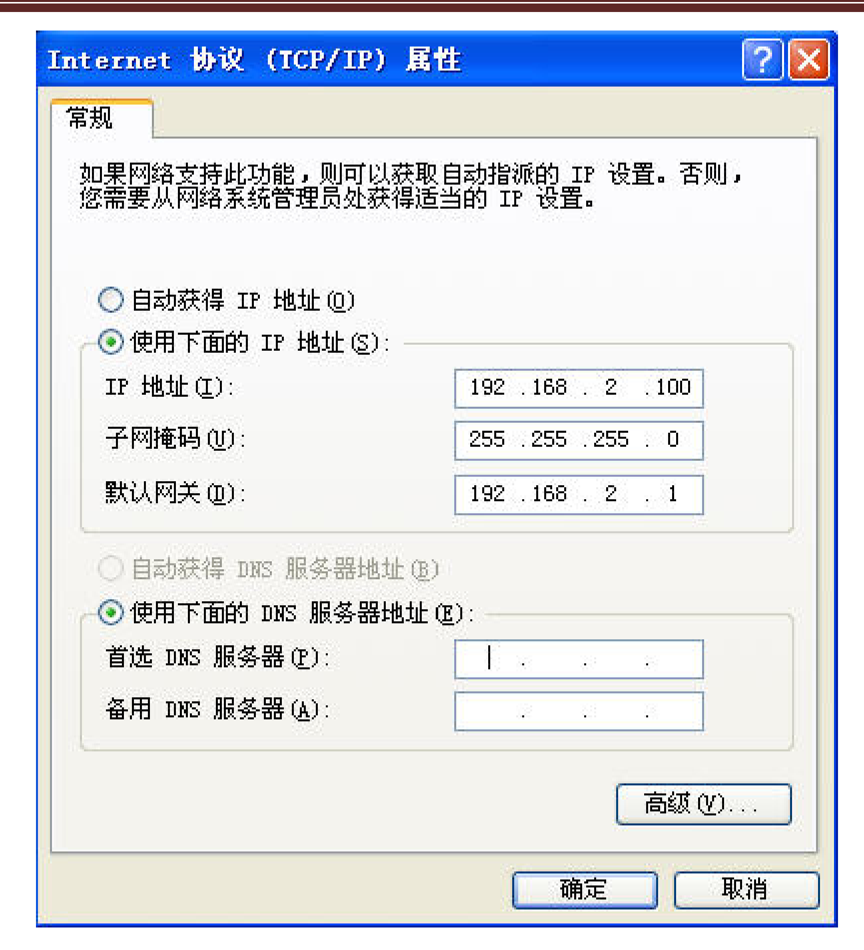


图 2.1 设置管理主机 IP 地址登录防病毒卡

当用户尝试登录管理界面时，会显示一个认证框。用户需要输入有效的用户名和密码以完成认证。有关如何在防病毒卡中添加用户账号请参阅本使用手册4.2 账号管理。

在浏览器地址栏中，输入 https://192.168.2.1（默认防病毒卡管理口的地址），浏览器会自动弹出一个安全警报，如图 2.2 所示。基于安全因素的考虑，防病毒卡通过 SSL 连接到管理站点。

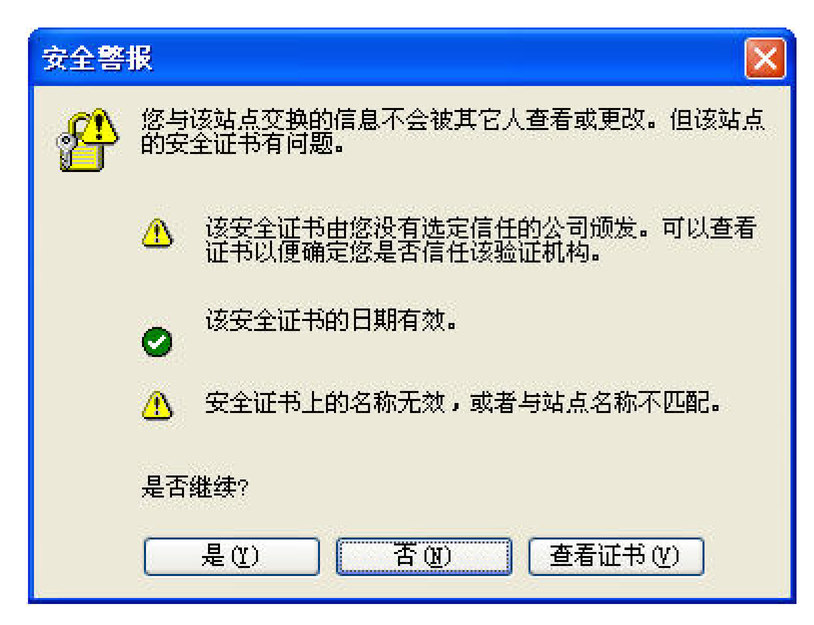
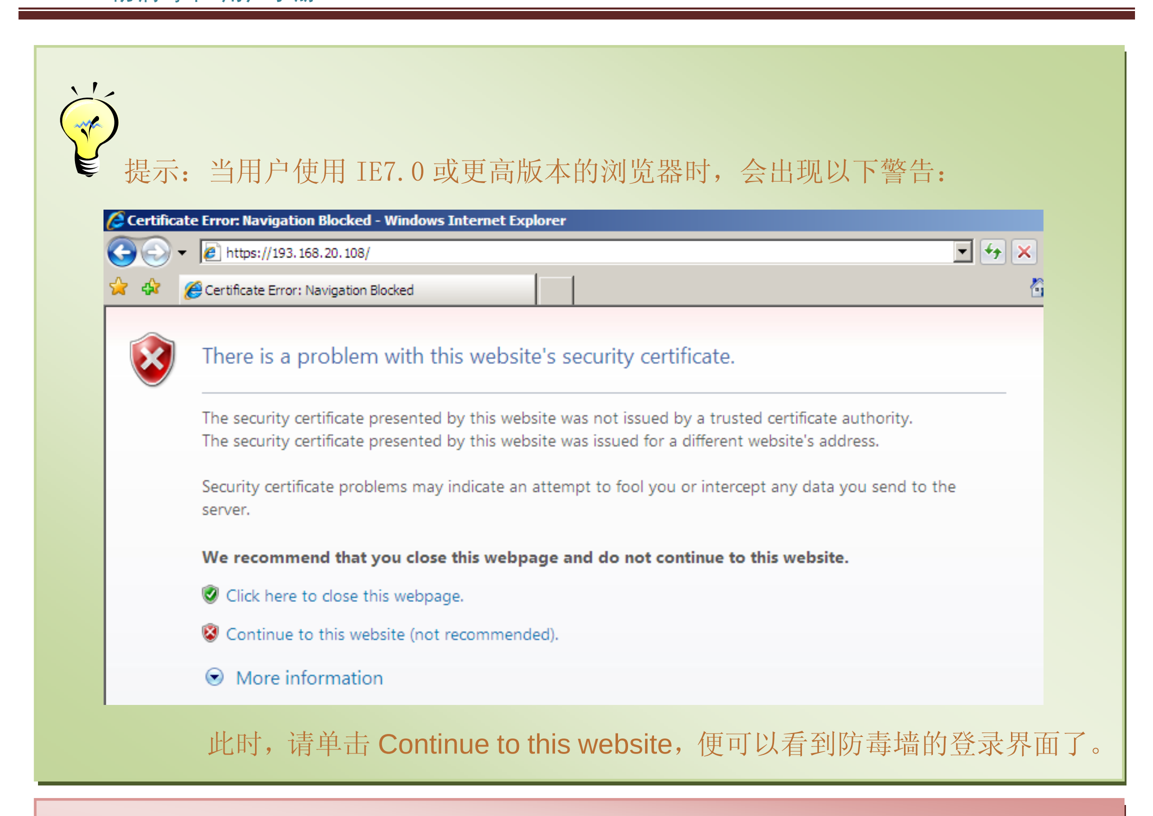


图 2.2 防病毒卡证书

提示：当用户使用 IE7.0 或更高版本的浏览器时，会出现以下警告：



此时，请单击 Continue to this website，便可以看到防毒墙的登录界面了。

注意：强烈建议登录后立即修改默认密码。如何修改防毒墙用户密码参阅本手册4.2 节帐号管理。

1. 选择信任证书，进入防病毒卡登录界面。如图 2.3 所示



图 2.3 防病毒卡系统登录界面

2. 在用户名栏中，输入用户名：“admin”

3. 在密码栏中，输入默认密码：“admin”

4. 单击【登录】按钮,进入防病毒卡网页管理界面，并显示当前防病毒卡系统信息。如图 2.4 所示



图 2.4 防病毒卡登录界面

2.2 防病毒卡功能菜单

防病毒卡管理菜单分为六项功能区域，每一个功能区域都由菜单区和主页面构成。

- 主页面：显示各个功能模块的管理页面。可对防病毒卡进行相关的配置
- 菜单区：弹出式菜单。鼠标悬停在菜单栏上，右侧会弹出二级子菜单。如图 2.5 所示



图 2.5 防病毒卡二级菜单

功能菜单	说明
系统配置	包括系统维护、接口配置模块
系统设置	包括远程管理、帐号管理模块
防毒管理	设置防毒规则以及病毒查杀行为
系统状态	显示当前防病毒卡的工作状态
安全审计	进行事件日志、安全日志的查看以及保存管理设置
退出	退出防病毒卡管理页面

表 2 防病毒卡的主要功能

第三章 系统配置的功能和使用

本章主要介绍以下两个模块的功能以及使用方法。

- 系统维护：备份配置信息、病毒库及系统升级的相关设置
- 接口配置：设置防病毒卡地址参数

3.1 系统维护

3.1.1 备份当前配置

单击【系统配置】➔【系统维护】，在备份信息对话框下输入备份信息供日后查询。如图 3.1 所示。



图 3.1 创建备份

单击【备份】，系统将防病毒卡的配置保存到一个文件中。如图 3.2 所示。



图 3.2 保存配置文件保存

单击【确定】，返回到系统维护页面，在刚才【备份】按钮旁将会出现【下载备份文件】按钮，如图 3.3 所示。

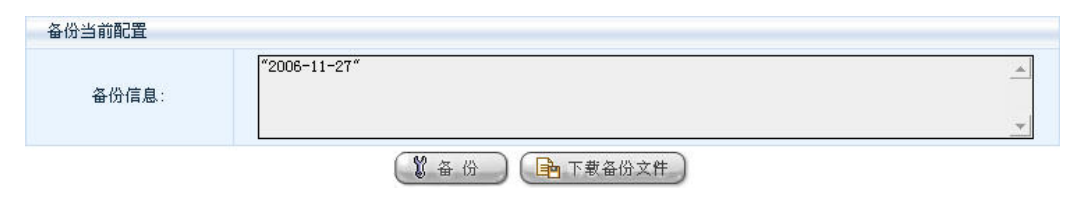


图 3.3 下载防病毒卡备份文件

单击【下载备份文件】将备份文件下载至本地计算机上保存。系统弹出另存备份文件对话框，如图 3.4 所示。

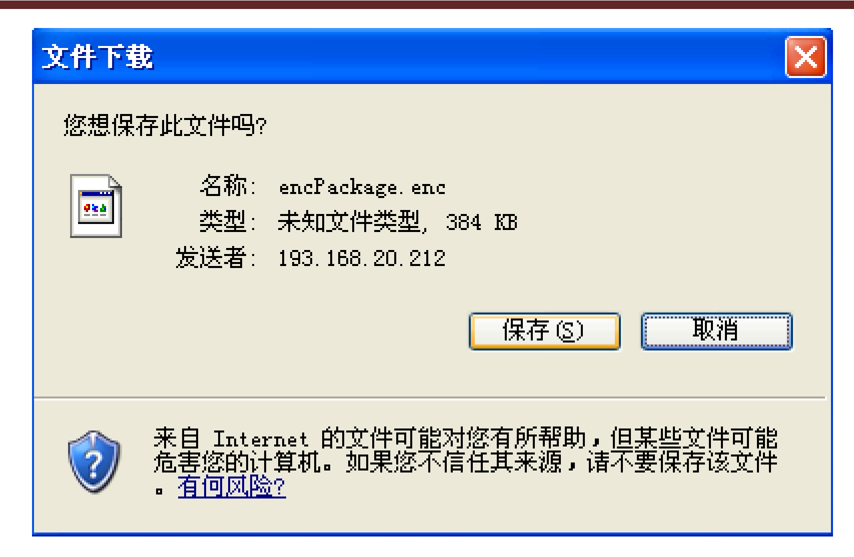


图 3.4 另存备份文件

选择保存目录，如图 3.5 所示。

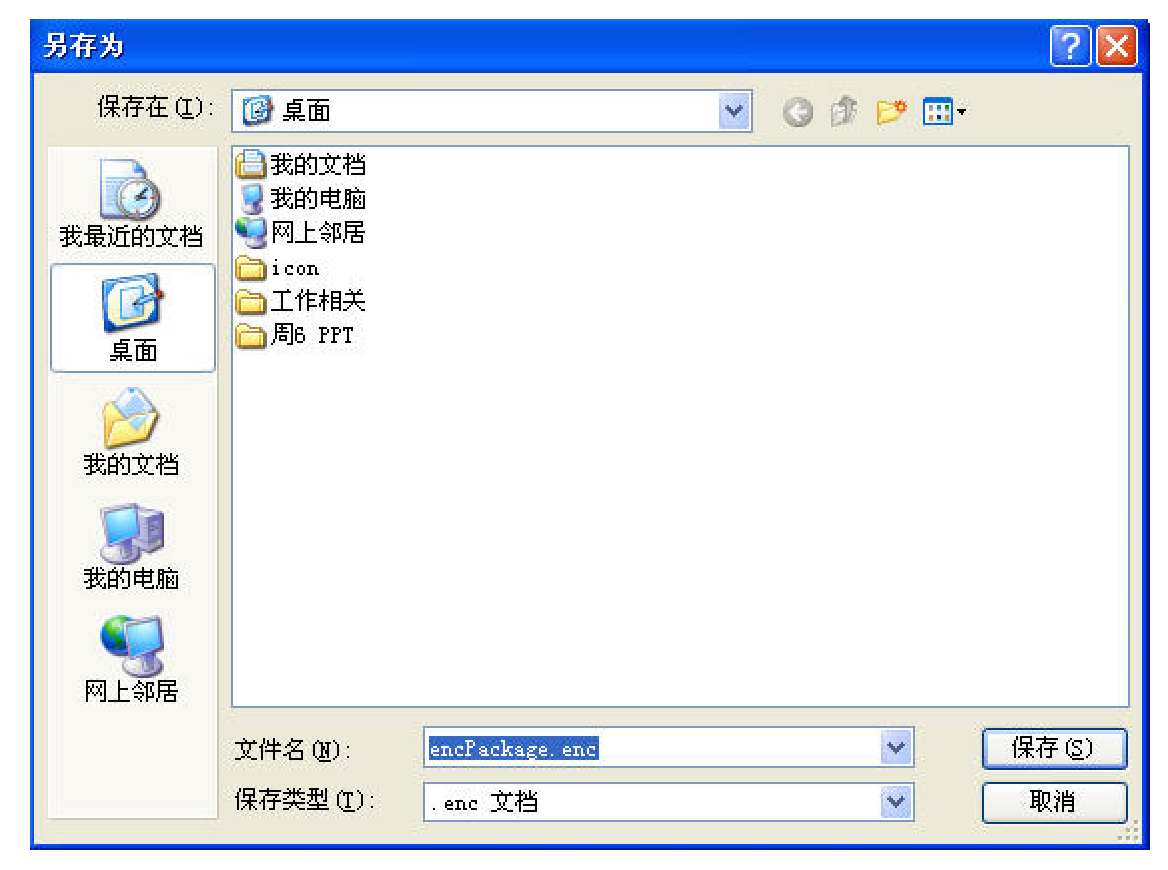


图 3.5 导出备份文件的位置

单击【保存】，保存防病毒卡配置。

3.1.2 恢复配置

使用备份文件恢复防病毒卡配置：

1. 单击使用备份文件恢复中的【浏览】按钮，选择存放配置文件的目录，如图 3.6 所示

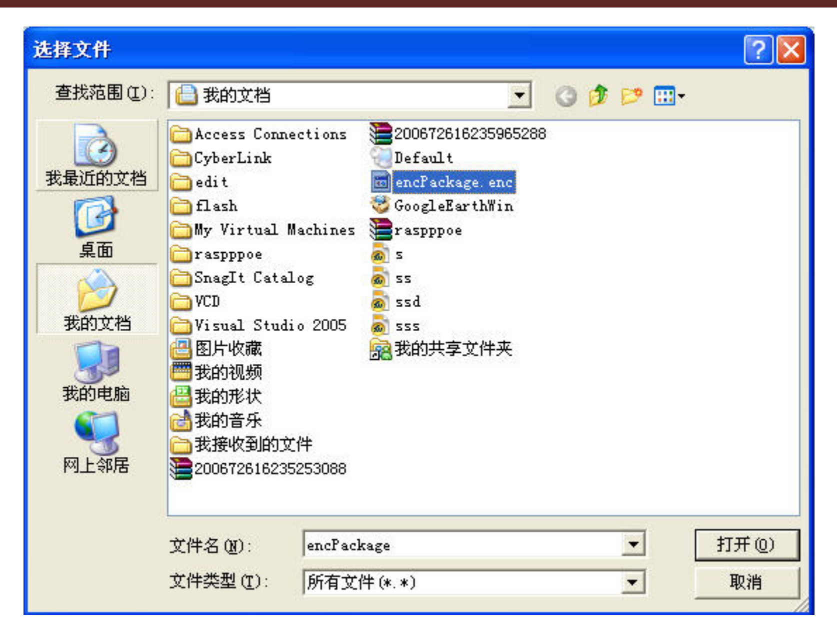


图 3.6 选择导入备份文件

2. 选择以往备份的文件，如图 3.7 所示

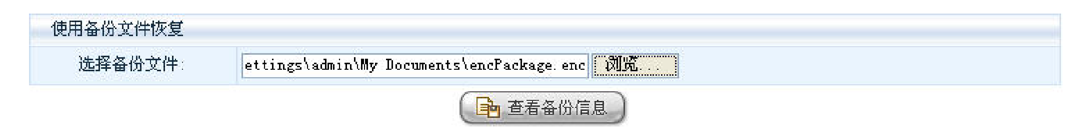


图 3.7 使用备份文件恢复系统设置

3. 点击【查看备份信息】可以看到当前备份文件包含的备份信息，如图 3.8 所示



图 3.8 查看备份信息

4. 单击【恢复】，使用选定的配置文件恢复系统配置

3.1.3 升级

防病毒卡升级分为系统升级和病毒库升级。

提示：在您对防病毒卡病毒库进行升级前，请您先对产品进行注册。

在病毒库升级部分，选择注册单选按钮。如图 3.9 所示。

病毒库升级	
您将要:	○ 手动升级病毒库 ○ 自动升级病毒库 ⦿ 注册
产品序列号:	- - -
注册状态:	无效序列号
有效日期:	未启用
病毒库版本:	/

注 册

图 3.9 注册病毒库升级许可

- 产品序列号：请从产品包装箱中的注册卡上查看产品的反病毒引擎序列号，并填入此栏。之后，单击【注册】按钮
- 注册状态：当前许可可用性。当成功注册后，会显示“已注册”
- 有效日期：许可的期限

3.1.3.1 病毒库升级

防病毒卡的病毒库升级有自动和手动两种模式。如图 3.10 所示。



图 3.10 防病毒卡病毒库升级设置

- 自动升级：通过设置病毒库自动升级的时间，防病毒卡系统通过网络自动下载升级包对病毒库进行升级。如图 3.11 所示

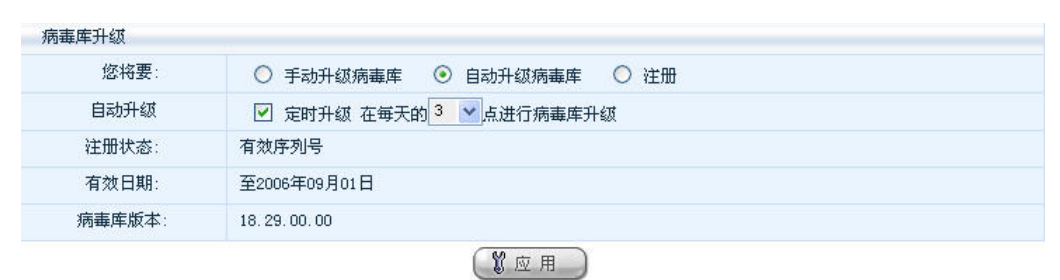


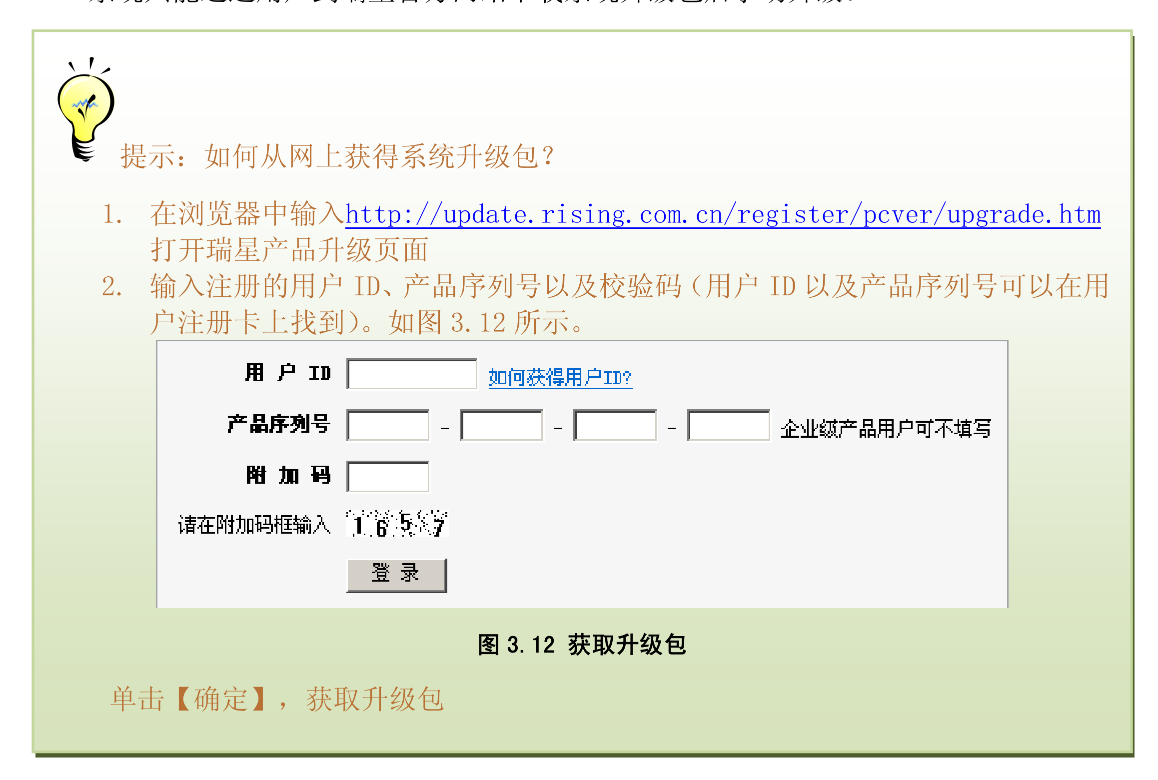
图 3.11 自动定时升级

- 手动升级：用户手动操作对防病毒卡进行升级。手动升级有三种方式，用户可根据实际情况进行选择
  - ✓ 网络升级：单击【应用】自动从瑞星网站下载最新的病毒库文件

- ✓ 本地局域网升级：将防病毒卡病毒库文件下载到同一局域网内的一台 HTTP 服务器，通过填写 HTTP 服务器的详细 URL 地址进行升级
- ✓ 本地升级：将病毒库升级包下载到本地，手动选择升级包进行防病毒卡病毒库的升级

3.1.3.2 系统升级

系统只能通过用户到瑞星官方网站下载系统升级包后手动升级。



提示：如何从网上获得系统升级包？

1. 在浏览器中输入http://update.rising.com.cn/register/pcver/upgrade.htm 打开瑞星产品升级页面
2. 输入注册的用户 ID、产品序列号以及校验码（用户 ID 以及产品序列号可以在用户注册卡上找到）。如图 3.12 所示。

图 3.12 获取升级包

单击【确定】，获取升级包

1. 单击【浏览】，选择升级文件所在目录。如图 3.13 所示

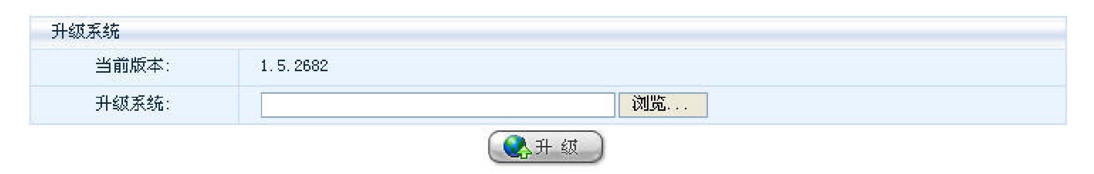


图 3.13 浏览升级文件目录

2. 选择升级文件。如图 3.14 所示

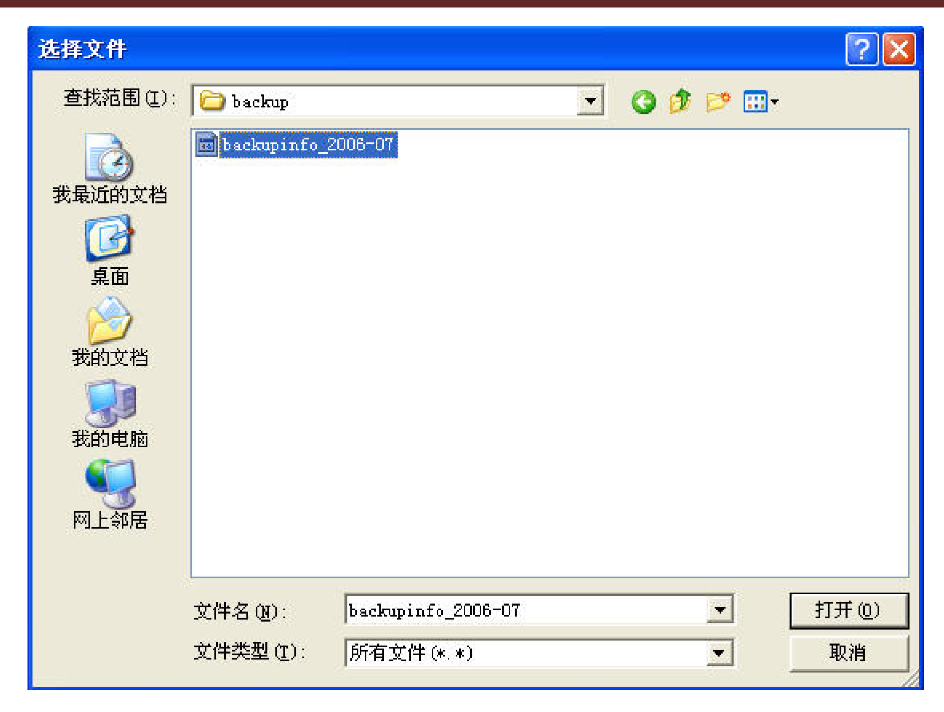
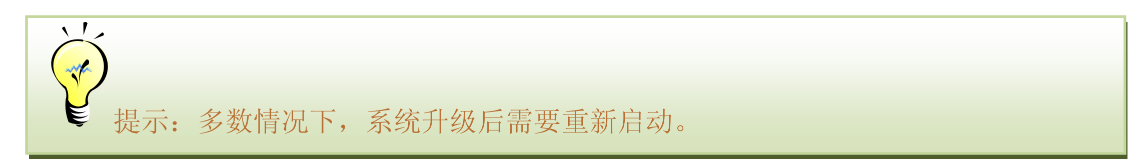


图 3.14 选择升级文件

3. 单击【升级】按钮



3.1.4 自动关闭系统

防病毒卡提供自动关闭系统的功能。在自动关机页面下，勾选单选框启用防病毒卡自动关机功能。您可以根据需要选择关闭防病毒卡时间，选择完自动关机的时间后单击【应用】按钮，保存设置。如图 3.15 所示。



图 3.15 定时关闭防病毒卡系统

3.1.5 恢复出厂设置

单击“恢复出厂设置”图标会出现一个对话框，询问是否将系统恢复到出厂状态，单击【确定】按钮将系统恢复到出厂状态，单击【取消】按钮放弃将系统恢复到出厂状态。如图 3.16 所示



图 3.16 恢复防病毒卡系统到出厂状态

3.1.6 关闭系统

单击“关闭系统”图标会出现一个对话框询问是否确定关闭系统，单击【确定】按钮将关闭系统，单击【取消】按钮放弃关闭系统。如图 3.17 所示。



图 3.17 关闭防病毒卡系统

3.1.7 重启系统

单击“重启系统”图标会出现一个对话框询问是否确定重启系统，单击【确定】按钮将重启系统，单击【取消】按钮放弃重启系统。如图 3.18 所示。



图 3.18 重启防病毒卡系统

3.2 接口配置

单击【系统配置】➔【接口配置】，进入防病毒卡接口配置页面，如图 3.19 所示。



图 3.19 防病毒卡接口配置

其中：

字段	说明
本地 IP 地址	这是为了防病毒卡可以和外部的网络设备（路由器、防火墙等）正常通信而设置的 2 个地址。
关联 IP 地址	
SNMP 接口配置	简单网络管理协议，通过此设置集中管理防病毒卡
管理 IP 地址 / 掩码	防病毒卡管理口的 IP 地址
默认网关	防病毒卡自身使用的网关地址（推荐用户设置为与“关联 IP 地址”相同，且不能配置为 0.0.0.0）

表 3 防病毒卡接口配置说明

3.2.1 防病毒卡接口配置

防病毒卡前面板的接口是管理接口。用来与网络设备进行数据交互的接口为内部接口。

- 防病毒卡上与网络设备进行数据交互的接口的地址称为本地 IP 地址。网络设备上与防病毒卡进行数据交互的接口的 IP 地址称为关联 IP 地址。因此，我们需要事先在网络设备上配置好与防病毒卡相连的接口的地址，再把这个地址填入到关联 IP 地址栏中。本地 IP 地址必须与关联 IP 地址处于同一网段，而且它们两个不能和管理 IP 地址处于同一网段。

- 将 SNMP 的用户名、授权密码和加密密码依次输入到 SNMP 接口配置下（保证与网络设备的正常通讯），单击【应用】按钮

- 管理接口地址配置是防病毒卡进行管理的唯一地址，修改时请谨慎操作！请牢记修改后的IP地址，以便日后配置管理防病毒卡。如果忘记防病毒卡管理IP地址，请通过串口修改管理IP地址（参阅附录一 串口管理）

第四章 防病毒卡管理设置

本章主要从两个方面介绍防病毒卡的管理设置：

- 远程管理
- 帐号管理

4.1 远程管理

远程管理功能中可以对管理员远程管理选项、接口访问限制和 IP 访问控制进行管理。防病毒卡的日常维护一般都是通过远程管理完成，这部分的配置对日后的维护工作非常重要。

4.1.1 远程管理选项

设置远程管理防病毒卡时的管理超时、自解锁时间和错误登录次数，如图 4.1 所示。



图 4.1 远程管理

- **管理超时**：设置管理超时时间，如果某一管理员登录超时，管理页面将弹出消息框提示“因管理超时被自动退出，如需管理请重新登录”，管理页面退回到登录页面
- **错误登录次数**：设置同一用户允许尝试登录的次数。如果超过允许尝试登录的次数而没有正确登录，管理页面将弹出消息框提示“该用户被锁定”，只有防病毒卡自解锁时间过后用户才能继续尝试登录
- **自解锁时间**：设置解除防病毒卡因超过允许尝试登录次数而锁定的 IP 地址的间隔时间。例如：自解锁间隔时间设置为 1 小时，防病毒卡锁定 1 小时之内该 IP 不能登录管理页面，1 小时后锁定自动解除，到时可以登录防病毒卡

4.1.2 接口访问控制

设定接口支持的管理方式，如图 4.2 所示。

接口访问控制

允许PING:	☐ 全部接口
	☑ 外网接口 ☑ 内网接口
允许Web管理:	☑ 全部接口
	☐ 外网接口 ☐ 内网接口
允许SSH管理:	☑ 全部接口
	☐ 外网接口 ☐ 内网接口

应 用

图 4.2 接口访问控制

其中：

字段	说明
允许 PING	是否允许网络上的主机通过 ICMP 协议探测防病毒卡的地址可达
允许 WEB 管理	是否允许用户通过 Web 进行防病毒卡管理

允许 SSH 管理	是否允许用户通过 SSH 协议连接到防病毒卡，并进行管理

表 4 防病毒卡接口访问控制

4.1.3 IP 访问控制

设置允许通过web管理的IP地址或地址段。

提示：IP 访问控制是基于接口管理控制的，即添加的 IP 范围必须在可允许的管理接口范围内才有效，防病毒卡默认是允许所有 IP 地址进行 web 管理。



图 4.3 IP 访问控制

如图 4.3 所示，允许 192.168.100.158，掩码为 255.255.255.255 的主机通过 web 页面管理防病毒卡。



注意：设置了 IP 访问控制列表后，只允许控制访问列表中存在的 IP 地址进行访问控制。

4.1.3.1 添加 IP 访问控制列表

单击 IP 访问控制页面的【增加】按钮，如图 4.4 所示。





图 4.4 增加 IP 访问控制地址

- 状态：选中“启用”框，则表示该策略生效
- 策略：分为“允许”和“拒绝”两种策略
- 网段：填写 IP 地址或网段。用户可以按照以下三种方式来指定地址：
  - 添加单一的 IP 地址：直接填写 IP 地址，例如：192.168.100.88
  - 添加一个网段：IP 地址/掩码的位数，例如 193.168.10.0/24
  - 添加一段 IP 地址：起始 IP 地址－结束 IP 地址，例如 193.168.10.1-193.168.10.10

4.1.3.2 修改 IP 访问控制列表

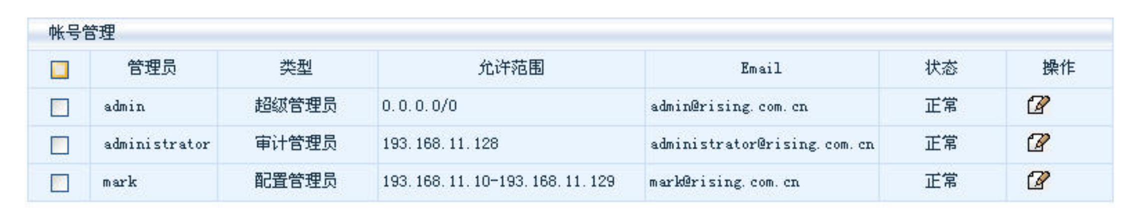
如果需要修改已存在的列表，请单击该记录的图标进入修改页面进行修改。

4.1.3.3 删除 IP 访问控制列表

如果需要删除已存在的列表，请单击该记录的🗑图标。

4.2 账号管理

防病毒卡的超级管理员可对帐号进行管理（增加、删除及修改），如图 4.5 所示。



帐号管理

	管理员	类型	允许范围	Email	状态	操作
☐	admin	超级管理员	0.0.0.0/0	admin@rising.com.cn	正常	
☐	administrator	审计管理员	193.168.11.128	administrator@rising.com.cn	正常	
☐	mark	配置管理员	193.168.11.10-193.168.11.129	mark@rising.com.cn	正常	



图 4.5 帐号管理

4.2.1 增加管理员帐号

单击【增加】按钮进入帐号增加页面，如图 4.6 所示。

增加管理员

用 户 名：	rising
密 码：	••••••
确认密码：	••••••
权 限：	审计管理员
地址范围：	○ 单个地址： ○ 地址/掩码： / ◉ 地址段： 193.168.11.12 - 193.168.11.16
电子邮件：	rising@rising.com.cn



图 4.6 增加管理员管理帐号

- 用户名：要添加的用户名
- 密码：添加的用户名的密码
- 确认密码：重新输入要设定的密码
- 权限：设定的账号拥有的权限
- 地址范围：指定可以管理防毒墙的IP地址，用户可以指定一个地址、一个网段或者一段地址，指定方法和4.1.3.1 添加IP访问控制列表中的相同

提示：IP 访问控制中的设定的优先级将高于添加管理员中的设定。如果这两个地方的设定有冲突，防病毒卡将以 IP 访问控制中的设定为准。

- 电子邮件：该账号使用的联系邮件

可用的管理员权限：

账号类型	说明
审计管理员	可以阅读部分防病毒卡设置，但不可以修改
配置管理员	可以阅读全部防病毒卡设置，可以进行部分设置的修
超级管理员	可以阅读全部防病毒卡设置，同时可以修改全部设置

表 5 管理员权限列表

设定好上述信息后，单击【增加】按钮完成管理员帐号的添加。同时，添加的管理员帐号会自动加入到管理员列表中。

4.2.2 修改管理员账号

单击某一条管理员记录的图标可以修改其密码、权限以及可访问管理的 IP 地址。如图 4.7 所示。



图 4.7 修改系统帐号权限

各部分的含义和添加用户帐号相同。

提示：只有超级管理员拥有全部帐号的修改和删除权限，而审计管理员和配置管理员对于帐号管理只有修改密码和源地址的权限。

4.2.3 删除管理员帐号

若要删除某个帐号，选中该帐号，然后单击【删除】按钮。（需要有超级管理员权限）。

第五章 防毒管理

防病毒卡支持邮件协议(POP3)、简单邮件传输协议(SMTP)、文件传输协议(FTP)和超文本传输协议(HTTP)的病毒查杀，可以实现查杀邮件附件、传输文件和网页内容中的病毒。

将上述协议的病毒扫描启用后，防病毒卡就自动扫描使用该协议传输的数据，并进行病毒检测。为确保防病毒卡能够检测最新的病毒，请您及时升级其病毒库文件。有关病毒库更新，可参阅本用户手册3.1.3.1 病毒库升级。

防病毒卡每检测出一个带毒文件都会对应地建立一个日志信息。

防病毒卡支持的防毒功能主要有：

- 防毒配置
- 防毒规则



提示：关于病毒查杀

- 受邮件代理所限，防病毒卡邮件扫描暂不支持 Unicode 编码。但由于目前绝大多数的邮件用户都设定成使用多目的因特网邮件扩展(MIME)编码，因此不支持 Unicode 编码几乎不会给您带来安全问题
- 防病毒卡可对 MSN，Hotmail 和 Yahoo 等基于网页的邮件系统进行有效地扫描
- 防病毒卡支持对最大为 25 层压缩的文件进行扫描
- 防病毒卡可扫描大部分压缩文件格式（.rar 和.ace 文件必须是由 WinRAR 3.0 或更高版本生成的）。当同时有大量的压缩文件附件到达时，可能会造成网络性能的下降
- 防病毒卡不能扫描带有密码保护的压缩文件

5.1 防毒配置

5.1.1 病毒查杀策略

单击【防毒管理】➔【防毒配置】，进入病毒查杀策略页面，如图 5.1 所示。



图 5.1 病毒查杀策略

病毒查杀策略分为“性能优先”和“准确性优先”。

- 性能优先：防病毒卡对满足防毒策略的数据进行杀毒处理，如果性能不足时（系统 CPU 占用率 100%或内存达到峰值）则对部分数据进行转发而不再进行病毒扫描查杀。即：当系统的性能达到设定的极限时，系统又接受到新的命令，此时系统将对剩下的数据不再进行查杀毒处理，而直接转发

- 准确性优先：防病毒卡对满足防毒策略的所有数据进行杀毒处理。当系统过于繁忙的时候，会出现排队现象

5.1.2 病毒查杀配置

5.1.2.1 病毒处置

可以选择“查毒”或“杀毒并阻断”操作。若设置为查毒，发现病毒后不做删除等处理，只在日志中记录。若设置为杀毒并阻断，则发现病毒后会进行清除，并在日志中记录。如图 5.2 所示。

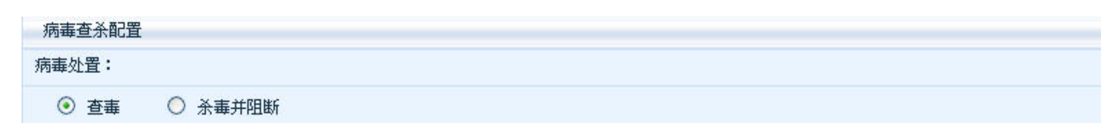


图 5.2 处理病毒方式

5.1.2.2 查杀文件大小设置

- 统一指定查杀文件的大小，若数据文件超过指定的大小将不做查杀，如图 5.3 所示

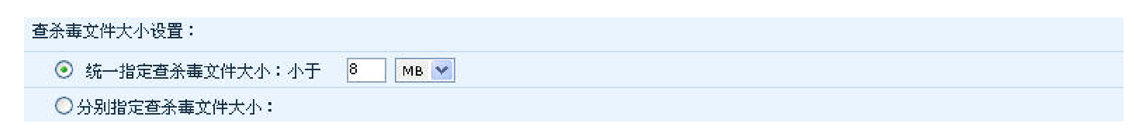


图 5.3 设置统一查杀文件的大小

- 分别指定查杀毒文件大小：对通过 HTTP、FTP、SMTP 及 POP3 四种协议传输的数据分别指定查杀文件的大小，若文件超过设置的大小将不做查杀。如图 5.4 所示

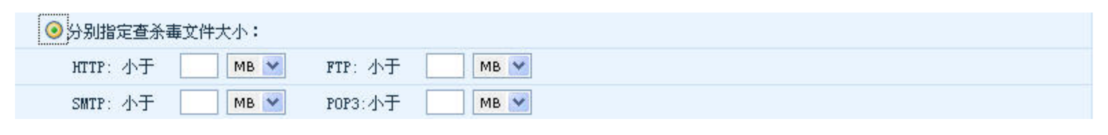


图 5.4 分别指定查杀文件大小

提示：查杀文件的大小以 MB 和 KB 为单位。当以 MB 为单位时：范围是 1-10 之间；当以 KB 为单位时，范围是 1-999 之间。

5.1.2.3 查杀类型

在查杀类型页面下可以选择查杀的文件类型，防病毒卡默认设置查杀常用的文件类型，用户在自定义文件类型下可定制对不常用的文件进行查杀。如图 5.5 所示。

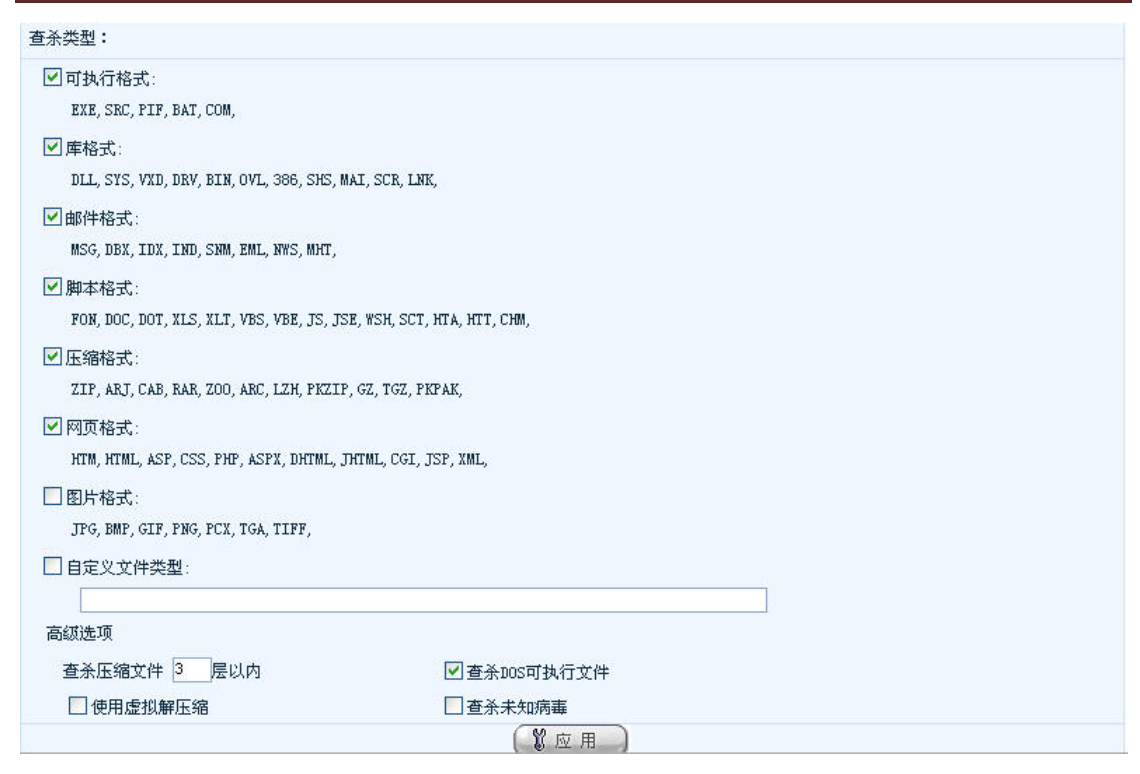


图 5.5 病毒查杀设置页面

- 可执行格式：对通过的后缀为 EXE、SRC、PIF、BAT、COM 格式的文件进行查杀
- 库格式：对通过的后缀为 DLL、SYS、VXD、DRV、BIN、OVL、386、SHS、MAI、SCR、LNK 格式的库文件进行查杀
- 邮件格式:对通过的后缀为 MSG、DBX、IDX、IND、SNM、EML、NWS、MHT 格式的邮件文件进行查杀
- 脚本格式：对通过的后缀为 FON、DOC、DOT、XLS、XLT、VBS、VBE、JS、JSE、WSH、SCT、HTA、HTT、CHM 格式的脚本文件进行查杀
- 压缩格式：对通过的后缀为 ZIP、ARJ、CAB、RAR、ZOO、ARC、LZH、PKZIP、GZ、TGZ、PKPAK 格式的压缩文件进行查杀
- 网页格式：对通过的后缀为 HTM、HTML、ASP、CSS、PHP、ASPX、DHTML、JHTML、CGI、JSP、XML 格式的网页文件进行查杀
- 图片格式：对通过的后缀为 JPG、BMP、GIF、PNG、PCX、TGA、TIFF 格式的图片文件进行查杀

5.1.2.4 高级选项

单击查杀类型页面上的【高级选项】可以进一步定义引擎的行为。

- 自定义文件类型：用户可以根据需要定义对其它后缀的文件进行扫描
- 查杀压缩文件：设置查杀几层压缩文件
- 查杀 DOS 可执行文件：对 DOS 下的可执行文件进行查杀
- 使用虚拟解压缩：对加壳的程序进行解压缩，应用此选项会增加系统负担
- 查杀未知病毒：对防病毒卡病毒库中没有记录的病毒进行查杀

5.1.3 协议设置

可以对常用的 HTTP 协议进行设置，禁止下级使用其它代理或非 HTTP 协议，也可以对通过 HTTP 协议上传文件的大小做出限制。如图 5.6 所示。

- 禁用下级代理：通过防病毒卡后的数据不能是指向一个代理服务器的数据
- 禁用非 HTTP 协议：启用此功能，防病毒卡会丢弃使用非 HTTP 协议的数据
- 限制上传文件的大小：限制通过 HTTP 协议上传文件的大小



图 5.6 防病毒卡 HTTP 协议设置

5.2 防毒规则

单击【防毒管理】➔【防毒规则】，查看和设置病毒查杀规则。如图 5.7 所示。



病毒查杀列表配置

	序号	状态	入口	出口	转发接口	源地址	目的地址	服务	策略	操作	移动
	1		InLoopBack0	NULL0	GigabitEthernet0/1	3.3.3.3	4.4.4.4	H80:F21:S25:P110			
	2		GigabitEthernet0/1	GigabitEthernet0/0	GigabitEthernet1/0	1.1.1.1	2.2.2.2	H80:F21:S25:P110			
	3		GigabitEthernet0/0	GigabitEthernet0/1	GigabitEthernet1/0	1.1.1.1	2.2.2.2	H80:F21:S25:P110			
	4		GigabitEthernet0/1	GigabitEthernet0/0	GigabitEthernet1/0	1.0.0.200/24	2.0.0.200/24	H80:F21:S25:P110			

设为启用　设为停用　增 加　删 除

图 5.7 病毒查杀列表配置

其中：

字段	说明
序号	按照阿拉伯数字排序，数字越小说明策略优先级越高
状态	图标说明策略为启用状态，图标说明策略为停用状态。
入口	定义进入此策略的数据流
出口	所有流出此策略的数据流
转发接口	将数据转发到此接口进行病毒检查，检查完毕后数据通过该接口返回
源地址	定义此规则的数据来源地址
目的地址	定义此规则的数据目标地址
策略	定义该策略的行为模式。在防病毒卡策略上共有两种行为模式：转发和不转发。绿色图标对勾表示转发，红色的图标为不转发
服务	说明此规则查杀何种服务内容，可以根据需要自定义服务的端口
操作	单击进入修改防毒规则页面
移动	移动调整定义的策略规则顺序
设为启用	开启某个被停用的策略，选中该策略前的复选框单击【设为启

	用】，则该策略被启用开始服务
设为停用	停用某个被启用的策略，选中该策略前的复选框单击【设为停用】，则该策略停止服务
增加	增加一条新的病毒查杀策略
删除	删除某条病毒查杀策略

表 6 查杀策略名词解释

5.2.1 移动病毒查杀策略顺序

防病毒卡的病毒查杀规则是有顺序性的，为了达到良好的效能，可以适当的调整策略次序以达到更好的网络查毒的效果。只要点击该规则移动栏内 "▼" 图案，即可进入顺序修改状态。如图 5.8 所示，点击第二条策略的▼操作按钮，在弹出的序号选择下拉框中选择要移动到的位置序号，就可以移动该策略的顺序。



	序号	状态	入口	出口	转发接口	源地址	目的地址	服务	策略	操作	移动
	1		InLoopBack0	NULL0	GigabitEthernet0/1	3.3.3.3	4.4.4.4	H80:F21:S25:P110			1
	2		GigabitEthernet0/1	GigabitEthernet0/0	GigabitEthernet1/0	1.1.1.1	2.2.2.2	H80:F21:S25:P110			1 2 3 4
	3		GigabitEthernet0/0	GigabitEthernet0/1	GigabitEthernet1/0	1.1.1.1	2.2.2.2	H80:F21:S25:P110			
	4		GigabitEthernet0/1	GigabitEthernet0/0	GigabitEthernet1/0	1.0.0.200/24	2.0.0.200/24	H80:F21:S25:P110			

图 5.8 移动病毒查杀策略的顺序

5.2.2 增加病毒查杀策略

单击【增加】按钮添加一条病毒查杀策略，如图 5.9 所示。

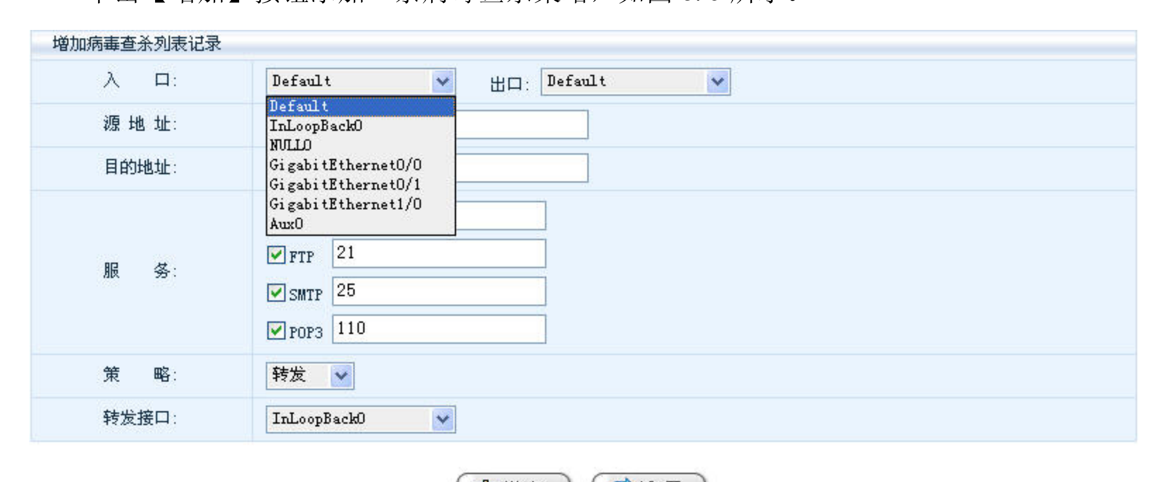


图 5.9 病毒查杀策略增加页面

其中：

字段	说明
入口	进入此策略的数据流。
出口	所有流出此策略的数据流。
源地址	定义该策略的数据来源地址。
目的地址	定义该策略的数据目标地址。

服务	该策略要检查何种服务内容。防病毒卡支持查杀通过 HTTP、FTP、POP3 和 SMTP 四种协议传输的数据，用户可根据需要自定义这四种服务的端口（也可对某种协议设置多个端口，添加多个端口请用逗号分隔）。上图 5.9 中所示服务端口号为该协议默认使用端口，适用于大多数的情况。
策略	该策略的行为模式。在防毒墙策略上共有两种行为模式：转发或不转发。转发为对数据进行检查，不转发则不进行检查。
转发接口	通过哪个接口进行数据转发。

表 7　病毒查杀策略说明

在该管理页面中的下拉框中选取入口、出口、源地址、目的地址、服务、策略以及转发接口，单击【增加】保存设置。

说明：

数据流的入口、出口均为 H3C 网络设备的三层以太网接口。

5.2.3　删除病毒查杀策略

若要删除某个策略，在病毒查杀列表配置页面选中该策略，单击【删除】按钮。

5.2.4　修改病毒查杀策略

如果需要修改已存在的病毒查杀策略，请点击该记录的修改图标进入修改页面进行修改。修改完毕后点击【确定】按钮保存修改的配置。如图 5.10 所示。

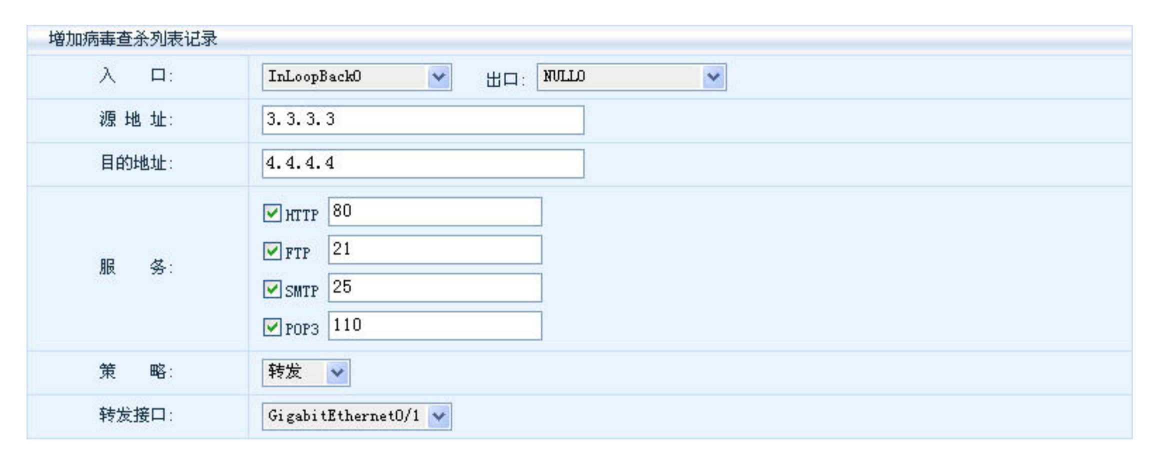




图 5.10 病毒查杀策略修改页面

第六章 系统状态

6.1 系统信息

显示系统当前的主要信息，如图 6.1 所示。当第一次打开该页面时会显示当时系统运行的情况，该信息每隔 4 秒刷新一次。CPU 和内存使用率反映出防病毒卡的系统负荷，系统运行时间显示当前系统正常运行时间。



提示：防病毒卡正常工作时 CPU 使用率不应超过 95%和空闲内存应大于 200M。

系统信息	
CPU使用率	0%
内存使用率 (148M/1011M)	14%
系统运行时间	0 天 5 小时 00 分钟 当前时间 (00:20:50)

图 6.1 防病毒卡系统信息

第七章 安全审计

本章我们从三个方面了解防病毒卡安全审计的详细设置：

- 事件日志
- 管理日志
- 日志保存设置

7.1 事件日志

事件日志用于记录防病毒卡检测到的各种网络攻击行为。

用户可以根据协议（HTTP、FTP、SMTP、POP3）源地址、目的地址、时间段或病毒名作为关键字对日志进行查找。如图 7.1 所示。



图 7.1 事件日志信息

防病毒卡事件日志支持两种查看方式

- 查看详细日志结果

选择查看方式中的查看详细记录结果选项，单击【搜索】按钮查看详细日志。可使用此功能查询防病毒卡拦截病毒的详细信息，如图 7.2 所示。



病毒日志详细信息 (共有1830条符合条件的记录)

序号	时间	协议	源IP	目的IP	描述	病毒名
11	2006-12-19 23:13:27	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/1_Trojan.Binghe2.0A.EXE	1:Backdoor.G_Door.20.a
12	2006-12-19 23:13:27	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/W32.Mincer.File.cab	1:Win32.Mincer
13	2006-12-19 23:13:27	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/PE_YAI.EXE	1:Win32.YAI
14	2006-12-19 23:13:27	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/1_Trojan.Binghe2.0A.cab	1:Backdoor.G_Door.20.a
15	2006-12-19 23:13:27	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/Win32.CTX.EXE	1:Win32.CTX
16	2006-12-19 23:13:26	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/Win32.CTX.cab	1:Win32.CTX
17	2006-12-19 23:13:26	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/Win32.Parite.c.EXE	1:Win32.Parite.c
18	2006-12-19 23:13:26	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/W32.Mincer.Vir.EXE	1:Win32.Mincer
19	2006-12-19 23:13:26	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/2_Trojan.G_Door.EXE	1:Trojan.G_Door
20	2006-12-19 23:13:26	HTTP	1.0.0.100	2.0.0.100	http://2.0.0.100/list/2_Trojan.G_Door.cab	1:Trojan.G_Door

首 页 上一页 下一页 末 页 [当前2/183页][下载日志信息]

图 7.2 病毒查杀日志的详细信息

其中：

字段	说明
序号	事件日志的序号
时间	事件的发生时间（以防病毒卡系统时间记录）
协议	通过何种协议进行传播

源 IP	数据包发送 IP 地址
目的 IP	数据包目的 IP 地址
描述	病毒信息的详细描述
病毒名	病毒的名称

表 8 病毒查杀日志记录说明

- 查看统计结果

选择查看方式中的查看统计结果选项，单击【搜索】按钮查看各种类型病毒的统计结果。通过这些统计信息，网络管理员能够直观查看病毒的出现几率，对于一些频繁出现的病毒，及时进行解决。如图 7.3 所示。

病毒日志统计信息(共有9条符合条件的记录)

序号	病毒名	出现次数	最早时间	最近时间	百分比
1	Win32.Nimda	1555	2006-12-19 23:09:16	2006-12-19 23:16:12	48.01%
2	Trojan.G_Door	313	2006-12-19 23:09:11	2006-12-19 23:13:28	9.67%
3	Win32.CTX	313	2006-12-19 23:09:16	2006-12-19 23:13:28	9.67%
4	Backdoor.G_Door.20.a	302	2006-12-19 23:09:10	2006-12-19 23:13:28	9.33%
5	Win32.Mincer	156	2006-12-19 23:09:15	2006-12-19 23:13:27	4.82%
6	Win32.Agent	156	2006-12-19 23:09:15	2006-12-19 23:13:27	4.82%
7	Win32.Mincer	154	2006-12-19 23:09:15	2006-12-19 23:13:27	4.76%
8	Win32.YAI	151	2006-12-19 23:09:15	2006-12-19 23:13:28	4.67%
9	Win32.Parite.c	139	2006-12-19 23:09:16	2006-12-19 23:13:26	4.3%

首 页 上一页 下一页 末 页 [当前1/1页][下载日志信息]

图 7.3 病毒查杀日志的统计信息

7.2 管理日志

管理日志包含所有关于防病毒卡配置的修改信息。每个日志条目都带有事件描述和日期时间戳。点击右下角的“下载日志信息”链接，系统日志将以 Excel 表格的形式下载到本地计算机，供日后对系统进行详细分析。

远程及本地管理接口登录失败将被记录在管理日志中。

管理日志

序号	时间	管理员	管理员类型	操作
1	10:35:59	admin [193.168.20.111]	超级管理员	admin用户登陆 : 成功!
2	10:33:52	admin [193.168.20.100]	超级管理员	admin用户管理超时，已退出
3	10:27:52	admin [193.168.20.111]	超级管理员	admin用户退出
4	10:22:09	admin [193.168.20.111]	超级管理员	admin用户登陆 : 成功!
5	10:03:48	admin [193.168.20.100]	超级管理员	admin用户登陆 : 成功!
6	09:15:51	admin [193.168.20.110]	超级管理员	admin用户登陆 : 成功!
7	09:15:03	admin [192.168.100.200]	超级管理员	admin用户登陆 : 成功!

首 页 上一页 下一页 末 页 [当前1/1页][下载日志信息]

图 7.4 管理日志操作信息

管理日志的查询:用户可以按“管理员”、“时间”及“操作”三种方式进行日志查询，如图 7.5 所示。



图 7.5 管理日志查询界面

7.3 日志保存设置

如果网络流量很大，系统日志增长较快。为防止日志大小超出硬盘容量，防病毒卡允许以本地 syslog 和 mysql、远程 syslog 和 mysql 四种方式记录日志。防病毒卡采用滚动日志机制,同时可设置日志的保存天数和磁盘占用百分比，超过保存天数或磁盘占用限额的日志文件将被自动删除。该功能确保防病毒卡不会因磁盘空间被日志占满而导致系统崩溃。

7.3.1 日志配置

- **本地日志**：本地日志分为 syslog 日志和 mysql 日志。防病毒卡默认会启动这两个日志。
- **远程日志**：防病毒卡的日志也可以备份到远程 syslog 服务器或 MySQL 数据库中
  - ✓ Syslog 远程记录日志：如图 7.6 所示。当选中启用复选框后，将出现远程 syslog 服务器的配置栏。

主机 IP	端口
远程 syslog 服务器的 IP 地址	Syslog 服务使用的端口号

表 9 syslog 服务器信息



提示：启用 syslog 远程记录日志前需要正确配置远程 syslog 服务器，并开启服务。

- MySQL 远程记录日志：如图 7.6 所示。当选中启用复选框后，将出现 MySQL 数据库的配置栏。

设置项目	说明
主机 IP	MySQL 数据库所在服务器的 IP 地址
端口号	MySQL 使用的端口号
用户名	登录 MySQL 数据库的用户名
密码	登录 MySQL 数据库的密码
数据库名	用于保存日志信息的数据库

表 10 MySQL 服务器信息

提示：启用 MySQL 远程记录日志前需要正确配置远程 MySQL 服务器，并开启服务。防病毒卡将在远程数据库上自动对服务器指定的数据库建表备份。



图 7.6 远程日志

7.3.2 本地存储控制

防病毒卡缺省设置为日志每日滚动一次，用户可以选择日志在防病毒卡上最多保存的天数以及最多占用磁盘空间的百分比，如图 7.7 所示。



图 7.7 日志保存设置

当设置完成后，单击【应用】按钮确认修改。

Appendix 1 串口管理

串口管理程序是当防病毒卡配置出现错误使系统无法正常工作时的补充手段，接通串口后将进入一个定制的 shell 环境，下面将要介绍有关的操作细节。

A1.1 登录串口

下面的步骤将介绍如何将防病毒卡设备与控制台进行连接。用串口线（RS-232 线）将控制台串口与防病毒卡串口连接好，然后在控制台上执行终端程序。以 Windows XP 系统下的超级终端程序为例：

1) 通过以下路径打开程序：【开始】➔【所有程序】➔【附件】➔【通讯】➔【超级终端】
2) 创建一个新的连接，输入连接名称并为连接选择一个图标，单击【确定】
3) 选择连接所用的串口，默认为 COM1
4) 在端口设置中选择如下属性，也可单击端口设置下【还原默认值】，使用默认设置
   - 每秒位数：　9600
   - 数据位：　8
   - 奇偶校验：　无
   - 停止位：　1
   - 数据流控制：　无
5) 单击【确定】创建连接。此时连接已建立，点击回车键显示登录信息，如下所示：

```
rising login: _
```

6) 输入登录用户名及密码，登录防病毒卡系统，此用户名及密码与 Web 管理界面的相同
7) 如果用户名及密码输入无误，将显示如下信息，表示已经登录成功，可以开始进一步管理操作

```
rising login: admin
Password:
[RsShell]$
```

A1.2 串口命令行列表

```
命令格式：?|help
```

示例：

```
?           show command list
help        show command list
exit        exit shell
reset       reset to default setting.
```

shutdown	shutdwon machine
reboot	reboot machine
repairdb	repair database
cron	configure scheduled task executed by crond daemon
upgrade	configure upgrade settings
ipaddr	show or configue interface IP address
route	static route configure
vscan	config virus scan
logconf	system log configure
logsave	set logsave configuration
logquery	display log
showsn	display device and engine Serial No.
time	display or set system time
support	config remote supporting

查看系统命令的帮助信息，用户可以根据帮助信息进行设置操作

命令格式： <基本命令> ? 或 help <基本命令>

示例：

```
[RsShell]$ reset ?
reset {system|config}
```

A1.3 串口命令

- **恢复出厂默认设置（reset）**

➢ **将系统恢复出厂状态**

命令格式：reset system

示例：

```
[RsShell]$ reset system
Reset will lose all current setting, do you want to reset to default setting? (y or n)
```

输入 y 按下回车键则系统恢复出厂状态，输入 n 按下回车键则放弃系统恢复出厂状态。

➢ **将系统设置恢复出厂默认设置**

命令格式：reset config

示例：

```
[RsShell]$ reset config
Reset will lose all current setting, do you want to reset to default setting? (y or n)
```

输入 y 按下回车键则系统恢复出厂设置，输入 n 按下回车键则放弃系统恢复出厂设置。


注意：以上两项操作会清空当前系统全部设置，请谨慎操作！

- **退出串口控制窗口（exit）**

命令格式： exit

- **接口 IP 地址 （ipaddr）**

查看或指定防病毒卡接口的 IP 地址

命令格式： ipaddr

示例：

```
[RsShell]$ ipaddr
eth1        193.168.20.212     255.255.255.0
lo          127.0.0.1          255.0.0.0
out         192.168.1.1        255.255.255.255
br0         192.168.1.1        255.255.255.255
```

添加或修改指定接口的 IP 地址

命令格式： ipaddr <iface> add ip mask

示例：将管理接口的的 IP 地址改为 192.168.50.50，掩码为 255.255.255.0。

```
[RsShell]$ ipadrr eth1 add 192.168.50.50 255.255.255.0
```

- **防毒管理（vscan）**

命令格式：vscan

```
[RsShell]$ vscan
scanaction=scanonly
max_size_http=8MB
max_size_ftp=8MB
max_size_smtp=8MB
max_size_pop3=8MB
exe_dos=on
zip_max_level=3
zip_veunpack=off
scanall=off
predefined_types=exe,lib,mail,script,zip,web
userdefined_types=
unknown_types=off
http_next_proxy=off
```

```
http_none_http=off
http_max_size_upload=10MB
http_virus_cache=on
```

- **病毒查杀策略**

  a） 查看当前策略

```
命令格式:vscan policy
[RsShell]$ vscan policy
performance
```

  b） 设置查杀策略为性能优先，即优先保证网络速度

```
命令格式： vscan policy performance
```

  c） 设置查杀策略为准确性优先，即优先保证查杀效果

```
命令格式： vscan policy veracity
```

- **病毒查杀配置**：病毒处置设置，设置对病毒的处理方法

  a） 设置为只扫描，即只对病毒进行检测而不清除

```
命令格式： vscan action scanonly
```

  b） 设置为扫描并杀毒，如果杀毒失败，则进行删除

```
命令格式： vscan action kill-delete
```

  c） 设置查杀文件大小，当文件小于该值时将不查杀，单位 M（兆）

  统一指定各协议查杀毒文件大小

```
命令格式： vscan file-max-size all <size>
```

  示例：将各个协议查杀文件大小限制为 10 兆。

```
[RsShell]$ vscan file-max-size all 10MB
```

  分别为 HTTP/FTP/POP3/SMTP 协议指定杀毒文件大小

```
命令格式： vscan file-max-size http|ftp|pop3|smtp <文件大小>
```

- **查杀文件类型设置**：系统将只查杀包含在设置中的文件类型

  1） 预定义文件格式：为方便用户定义防病毒卡查杀文件类型，系统内部设定了部分预定义文件格式组，包括 exe、lib、mail、script、zip、pic、web，可直接调用。同时调用多个时请用逗号（,）分隔

  2） 设定预定义文件格式

```
命令格式： vscan file-type predefined on <预定义文件格式>
```

  示例：设置对 exe、mail、zip 格式的文件进行查杀。

```
[RsShell]$ vscan file-type predefined on exe,mail,zip
```

  3） 添加预定义格式

注意：使用该命令后，原有的预定义格式设置将被清除。如果需要在当前设置基础上添加格式，请使用下面的添加命令。

命令格式： vscan file-type predefined add <预定义文件格式>

示例：添加对 web、script 格式的文件进行查杀。

```
[RsShell]$ vscan file-type predefined add web,script
```

4） 删除预定义格式

命令格式： vscan file-type predefined del <预定义文件格式>

5） 关闭所有预定义格式，即不对任何预定义格式中的文件类型进行查杀

命令格式： vscan file-type predefined off

6） 查杀 DOS 可执行文件功能开关

命令格式： vscan file-type predefined exe-dos on|off

7） 压缩文件最高查杀层数设定

命令格式： vscan file-type predefined zip-level <查杀层数>



注意：必须在查杀类型中添加预定义格式 zip，该设置才能生效。

8） 虚拟解压缩功能功能开关

命令格式： vscan file-type predefined veunpack on|off

- **设置自定义的文件类型**

对于没有包含在预定义格式里的文件类型，我们可以通过自定义文件类型功能进行设置查杀。

a） 设定自定义文件类型，如有多种格式请用逗号分隔

命令格式：vscan file-type user-defined on <文件类型>

示例：设定系统查杀 PSD、PDF 文件。

```
[RsShell]$ vscan file-type user-defined on psd,pdf
```

注意：使用该命令后，原有的自定义类型设置将被清除。如果需要在当前设置基础上添加文件类型，请使用下面的添加命令。

b） 添加自定义文件类型

命令格式： vscan file-type user-defined add <文件类型>

示例：添加 AI、CDR 文件到自定义查杀文件类型项中。

```
[RsShell]$ vscan file-type user-defined add ai,cdr
```

c） 删除自定义文件类型

命令格式： vscan file-type user-defined del <文件类型>

d) 关闭自定义文件类型，即不设置任何自定义文件类型

命令格式： vscan file-type user-defined off

e) 查杀未知病毒功能开关

命令格式：vscan file-type unknown on|off

- HTTP 协议设定

a) 是否禁用下级代理，on 表示不禁用，off 表示禁用

命令格式： vscan http next-proxy on|off

b) 是否禁用非 http 协议，on 表示不禁用，off 表示禁用

命令格式： vscan http none-http on|off

c) 是否启用杀毒缓存功能，on 表示启用，off 表示不启用

命令格式： vscan http virus_cache on|off

d) 设定上传文件大小限制，单位为兆字节(MB)，最大可以设定至 999MB。当设定值为 0 时，表示不限制上传文件大小

命令格式：vscan http upload-max-size <文件大小值>

示例：设定 http 协议最大上传文件体积为 6MB。

```
[RsShell]$ vscan http upload-max-size 6
```

- 日志管理（logconf）

- 查看当前日志管理配置

命令格式： logconf

示例：

```
[RsShell]$ logconf
local documentary log: enable
local database log: enable
remote documentary log: disable
remote database log: disable
```

- 远程日志设置

1） 开启/关闭远程 syslog 日志

命令格式： logconf remote file enable|disable

2） 开启/关闭远程 MySQL 日志。

命令格式： logconf remote database enable|disable

3） 设置远程 syslog 日志服务器登录项

命令格式： logconf remote file enable <主机地址> <主机端口>

4） 设置远程 MySQL 日志服务器登录项

命令格式：logconf remote database enable <主机地址> <主机端口> <登录用户名> <登录密码> <数据库名称>

示例：开启远程 MySQL 日志功能，并将远程主机地址设为 192.168.100.1:3306，登录用户名为 rising，密码为 rising，数据库名为 firewall。

```
[RsShell]$ logconf remote database enable 192.168.100.1 3306 rising rising firewall
```

- **管理设置（padmin）**

➢ 远程管理选项

a) 设置管理超时，允许错误登录次数，以及管理员帐号锁定后的自动解琐时间，时间单位为分钟

命令格式： padmin remote <timeout> <trytime> <autounlock>

示例：设置管理超时时间为 200 分钟，错误登录次数为 5 次， 自解锁时间为 20。

```
[RsShell]$ padmin remote 200 5 20
```

b) 查看当前管理设置

命令格式： padmin remote

示例：

```
[RsShell]$ padmin remote
Timeout: 200m
Autounlock: 20m
Trytimes: 5
```

➢ 接口访问控制

a) 查看当前接口访问控制配置

允许 PING 远程接口访问，运行命令：

```
padmin interface ping enable-all
```

允许 Web 管理远程接口访问，运行命令：

```
padmin interface web enable-all
```

允许 SSH 管理远程接口访问，运行命令：

```
padmin interface ssh enable-all
```

示例：

```
[RsShell]$ padmin interface
PING: all
WEB: all
SSH: all
```

b) 设置接口的管理访问权限

```
命令格式： padmin interface ping|web|ssh add|del <接口>
```

示例：

添加内网接口通过 Web 方式的管理访问权限。

```
[RsShell]$ padmin interface web add eth1
```

删除外网接口通过 SSH 方式的管理访问权限。

```
[RsShell]$ padmin interface ssh del eth0
```

➢ IP 访问控制

a) 查看当前允许管理访问的 IP 地址规则列表，当列表为空时表示允许任何 IP 地址访问

```
命令格式： padmin host
```

示例：

```
[RsShell]$ padmin host
    ID      Enable          Allow           Host Addr
    101     true        true        192.168.50.1
    102     true        true        192.168.50.5
```

1） 添加 IP 地址管理访问规则，此操作只能添加网段而不能添加单个 IP 地址。

```
命令格式： padmin host add <IP 地址/掩码>
```

示例：添加 193.68.60.0/24 网段到管理访问规则列表。

```
[RsShell]$ padmin host add 193.168.60.0/24
```

2） 从 IP 地址管理访问规则中删除，此操作只能通过规则 ID 进行，规则 ID 可以通过上边的查看列表命令查看。

```
命令格式： padmin host del <规则 ID>
```

示例：删除 ID 为 102 的访问规则。

```
[RsShell]$ padmin host del 102
```

- 关闭系统（shutdown）

```
命令格式： [RsShell]$ shutdown
Confirm to shutdown the machine? (y or n)
```

输入 y 按下回车键则关闭系统，输入 n 按下回车键则放弃关闭系统。

- 重启系统（reboot）

```
命令格式： [RsShell]$ reboot
Confirm to reboot the machine? (y or n)
```

输入 y 按下回车键则重启系统，输入 n 按下回车键则放弃重启系统。

- 设定计划任务（cron）

➢ 查看当前已设定的计划任务

命令格式： cron

示例：

```
[RsShell]$ cron
upgrade 0 21 * * * /etc/filter/upgrade.sh 2
```

系统能添加的计划任务包括定时升级（upgrade）和自动关机（shutdown）。

➢ 添加/修改计划任务

命令格式： cron shutdown|virus-upgrade on <时间参数>

示例：为系统添加每年一月 2 日 3 时 4 分自动关机的计划任务。

```
[RsShell]$ cron virus-upgrade on 4 3 2 1 a
```

➢ 删除计划任务

命令格式： cron shutdown|virus-upgrade off

时间参数：时间参数采用 Linux/Unix 格式，由 5 个由空格分隔的数字组成，从左至右分别表示分钟、小时、日期、月份、星期，表示的是一个时刻。例如一月 2 日 3 时 4 分星期五就可以表示为 4 3 2 1 5，当系统时间为这个值的时刻，相应的操作将执行。对于不确定的项，添加的时候用“a”补足，显示的时候则用“*”补足。

● 病毒库升级（upgrade）

命令格式： upgrade virus auto

● 日志本地储存控制（logsave）

➢ 查看当前日志储存设置

命令格式： logsave

设置日志占磁盘限额（单位：%）与日志保存时间（单位：天）

命令格式： logsave <磁盘限额> <保存时间>

示例：将系统的日志磁盘限额改为 80%，日至保留时间改为 180 天。

```
[RsShell]$ logsave 80 180
```

➢ 日志查询

1） 查询管理日志

命令格式：logquery <用户> <开始时间> <结束时间>

示例：查询 admin 帐号 2006 年 8 月 28 日 16 时至 2006 年 8 月 29 日 0 时的所有管理日志

```
[RsShell]$logquery admin 2006-08-28_16:00:00 2006-08-29_00:00:00
rows=2
|2006-08-28 16:18:30|rising|user|info|httpd|(null)|admin|3|193.168.11.45|admin 用户管理超时，已退出。
|2006-08-28 16:40:25|rising|user|info|httpd|(null)|admin|3|193.168.11.84|admin 用户登录，成功。
```

2） 查询事件日志

命令格式：logquery virus {ftp|http|pop3|smtp|all} <开始时间> <结束时间>

示例：查询 2006 年 8 月 24 日至 2006 年 8 月 29 日所有通过 http 查杀的事件日志。

```
[RsShell]$ logquery virus http 2006-08-24 2006-08-29

rows=145

|2006-08-24
    11:34:22|rising|user|notice|(squid)|(null)|0.0.0.0|148.110.168.192|323226382
    9|HTTP|http://192.168.110.149/nimda.zip|454049658|

|2006-08-24
    11:34:23|rising|user|notice|(squid)|(null)|1.0.0.0|148.110.168.192|323226382
    9|HTTP|http://192.168.110.149/nimda.zip|454049658|

|2006-08-24
    11:34:25|rising|user|notice|(squid)|(null)|2.0.0.0|148.110.168.192|323226382
    9|HTTP|http://192.168.110.149/nimda.zip|454049658|

|2006-08-24
    11:35:07|rising|user|notice|(squid)|(null)|10.0.0.0|148.110.168.192|32322638
    29|HTTP|http://192.168.110.149/nimda.zip|454049658|

--More-- (7% of 20344 bytes)
```

Appendix 2 专业术语表

A

安全套接层(SSL)

SSL 为 Secure Sockets Layer 的缩写，是一种基于允许加密和授权的互联网通讯协议。SSL 运行于 TCP/IP 之上。

管理账号

管理账号提供对防病毒卡管理界面不同级别的控制操作。

J

简单网络管理协议(SNMP)

SNMP 为 Simple Network Management Protocol 的缩写，是一种通过网络监测和管理远程设备的协议。SNMP 是专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议。 SNMP 使网络管理员能够管理网络效能，发现并解决网络问题以及规划网络增长。通过 SNMP 接收随机消息（及事件报告）网络管理系统获知网络出现问题。

W

网络掩码

网络掩码是一种 32 比特以小数点标记的符号，它允许路由设备区分一个 IP 地址的网络部分和主机部分。

例如：255.255.255.0 代表网络掩码 11111111.11111111.11111111.00000000，这表示地址的前 24 比特为网络地址，后 8 比特为主机地址。

文件传输协议（FTP）

FTP 为 File Transfer Protocol 的缩写，即文件传输协议，是一个用于简化 IP 网络上系统之间文件传送的协议， 采用 FTP 协议可使 INTERNET 用户高效地从网上的 FTP 服务器下载大信息量的数据文件， 将远程主机上的文件拷贝到自己的计算机上。以达到资源共享和传递信息的目的。FTP 使用客户方的某个随机接口的 TCP，与服务方的端口 21 相连接。

Y

域名系统(DNS)

DNS 是 Domain Name System（域名系统） 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，建立域名与 IP 地址一一映射的关系。

Z

兆比特每秒(Mbps)

1Mbps 表示每秒 1,000,000 字节。

子网

一个单独 IP 地址的再分。子网是通过屏蔽地址中最重要的字节，只保留其中独一无二的部分完成的。

Appendix 3 FAQ

A3.1 系统配置部分

Q：系统备份后，该如何进行防病毒卡的恢复工作？

A：对系统备份后，进行恢复前应首先将防病毒卡进行恢复出厂设置，然后进行系统恢复。

Q：如何判断系统是否升级成功？

A：系统升级成功，界面上会提示用户重启系统生效，同时在重新启动防病毒卡后，会在系统维护中显示新的版本号。在管理日志里可以看到升级到 XXXX 版本的日志，如果开启了远程 mysql 日志，在远程 mysql 日志的 adminlog 表也可以查到。

A3.2 系统管理部分

Q：更改防病毒卡远程管理下IP访问控制后，防病毒卡不能进行正常的远程管理？

A：防病毒卡默认允许所有地址对防病毒卡进行访问，如果添加了错误的 IP 访问地址，只有将进行远程管理的工作站计算机 IP 地址与添加 IP 访问地址配置在相同一个网段，如果忘记了添加的访问 IP 地址，只有进行串口登录更改可以访问的 IP 地址。

Q：远程管理选项中 3 个选项的数值范围各是多少？

A：“管理超时”的范围是 5—30 分钟；“错误登录次数”的范围是 4—10 次；“自解锁时间”的范围是 10—60 分钟。

Q：远程管理中“错误登录次数”设为 N 时，错误登录次数达到 N 时，并不提示“用户帐号已被锁定”？

A：“错误登录次数”设为 N 时，错误登录次数达到 N 时，该用户帐号已经被锁定，只是未提示，当进行第 N+1 次登录时，系统会提示“该用户已被锁定”。

Q： IP 访问控制中添加 IP 限制页面中的“网段”是什么格式？

A：“添加 IP 限制”页面中的“网段”填写格式为‘0.0.0.0/0’或‘192.168.10.0/24’。

Q：使用已设置的帐号登录系统时，提示“用户所处的 IP 无效”？

A：帐号管理表的允许范围（即地址范围）依赖于 IP 访问控制表中“IP/mask”一栏的设置。要想帐号生效，则帐号的允许范围必须在“IP/mask”一栏的 IP 地址范围内。

Q：同一个管理帐号是否可以同时在不同的 IP 登录到防病毒卡？

A：可以。

A3.3 防毒管理部分

Q：防病毒卡可以查杀几层压缩文件？

A：防病毒卡支持查杀 25 层压缩文件并对病毒予以清除。

Q：自定义病毒查杀文件类型是否可以包含 > < & 字符？

A：“>、<、&”等属于特殊字符,不允许添加。

Q：为什么病毒查杀列表配置列表中移动规则的顺序时提示错误？

A：如果病毒查杀列表配置中的某条配置不是最新，此时如果改变列表的排序，就会弹出错误窗口。正确做法是：选择所有的列表信息，单击设为【启用按钮】，系统就会自动更新列表信息，并把不是最新的信息删除。

Q：查杀病毒只支持通过 http、ftp、pop3 和 smtp 四种协议传输的数据吗？

A：目前只有这 4 种协议。因为我们检测到的病毒，绝大多数利用这 4 种协议进行传播。随着病毒可利用协议的增加，我们也会增加相应的功能。

Q：蠕虫病毒、木马和间谍软件，是否可以防止传播和查杀？

A：蠕虫、木马、间谍软件等都属于我们广义的病毒范围，全部在查杀范围以内。

A3.4 安全审计部分

Q：邮件附件中的病毒数超过 10 个，而防病毒卡的病毒日志详细信息中却只记录 10 个？

A：系统设定只显示 10 条日志记录。

Q：邮件的附件中含有多个病毒时，病毒查杀配置设为查毒时，在病毒日志详细信息中只记录 1 个病毒名？

A：在查杀邮件病毒时，系统设定只要查到病毒就不再继续查毒。

Q：我不知道病毒全名，怎么搜索相关的病毒日志？

A：可以填部分病毒名，搜索相关的信息。

Q：为什么远程 Mysql 服务器不能收到数据？

A：检查防病毒卡和远程 Mysql 服务器是否连通；查看 Mysql 用户名，密码是否和设置相对应；查看 Mysql 是否有远程访问的权限。

Q：怎么设定 Mysql 具有远程访问的权限？

A：在安装 MySql 后只有一个超级管理权限的用户 ROOT，而且 ROOT 限制只能在数据库本机上使用。如果我们要远程管理 MySql 该如何进行，事实上我们需要添加一个具有超级管理权限并且可能远程访问的超级用户。而在 MySql 中有两种方法可以实现这个目的，我们以增加一个超级权限管理用户 admin 为例来说明。

解决方法：

1. 改表法。可能是你的帐号不允许从远程登录，只能在 localhost 登录。这个时候只要在 localhost 的那台电脑，登入 mysql 后，更改“mysql”数据库里的“user” 表里的“host”项，从“localhost”改成“%”

```
mysql>use mysql;
mysql>update user set host = ‘%’ where user = ‘root’;
```

2. 授权法。例如，你想 admin 使用 something 从任何主机连接到 mysql 服务器

```
mysql>use mysql;
mysql>grant all privileges on *.* to ‘admin’@‘%’ identified by ‘something’ with grant option;
```

如果你想允许用户 root 从 ip 为 192.168.1.3 的主机连接到 mysql 服务器，并使用 something 作为密码

```
mysql>use mysql;
```

mysql> grant all privileges on *.* to ‘admin’@‘ 192.168.1.3’ identified by ‘something’ with grant option;